There is no I-32 document

TOP SECRET "U" TICOM/I-33

Report on Traffic Analysis of BAUDOT traffic.

by Capt. Jack Magilavy, A.U.S. and
D.R. UZIELLI, SIXTA

TICOM
9 July, 1945.

Copy No. 24
No. of Pages 4

DISTRIBUTION

British
1. Director
2. D.D.3
3. D.D.4
4. D.D.(N.S.)
5. D.D.(MW)
6. D.D.(A.S.)
7-8. A.D.(C.C.R.)(2)
9. Lt. Col. Leathem

U.S.
25-26. OP 20-G (2)(via Lt.Pendergrass)
27. G-2(via Lt. Col. Hilles)
28-29. S.S.A.(2)(via Major Seaman)
30-31. Director, S.I.D. ETOUSA(2)(via Lt.Col. Johnson)

TICOM
10. Chairman
11-12. S.A.C.(2)
13. Cdr. Bacon
14. Cdr. MacKenzie
15. Cdr. Tandy
16. W/Cdr. Oeser
17. Lt. Col. Johnson
18. Maj. Seaman
19. Lt. Eachus
20. Lt. Vance
21. Capt. Cowan
22. Lt. Feal
23-24. Ticom Files (2)

Additional
32. Major Wills

Do NOT Destroy. Return to the NSA Technical Library when no longer needed
5-4533
Copy No. 24

DECLASSIFIED
Authority NND 963016
By NR NARA Date 4-27

REPRODUCED AT THE NATIONAL ARCHIVES

Report on T/A of BAUDOT traffic. 8 July 1945

Prepared by: Capt. Jack Magilavy, A.U.S. and D.P. UZIELLI, SIXTA

1. The observations contained in this report are based on a comparatively short period of operation. Despite the small amount of material available, enough was at hand to permit certain definite conclusions to be drawn as to the correct approach to a T/A problem, which, in its essentials, is the same as the Russian Morse problem. Gaps in deductions were filled in by the Auswerter Karrenberg.

2. It was found that the message preambles and endings in themselves provide a wealth of material for analysis and in addition, the Russian Operators, like others, were inclined to be somewhat insecure in their chat. (As a result of the latter, three positive station identities were obtained).

3. The following are a sample preamble and ending -- broken down into their component parts, with pertinent remarks:

PREAMBLE

1	2	3	4	5	6	7	8a	8b	8c	9
AZBEST	451	/1	3/129		3/7	1150	SHO	ZVYEZDA	SHIFROVKA	15019

(1) ORIGINATING STATION. Cover names, changed at irregular intervals of from 3 to 14 days, are used instead of call/signs. These names are retained by the net and reshuffled after each change, e.g.; Moscow uses the cover name "Apple", Krakow "Beans", and Rostov "Carrots" for the period 9/7 to 13/7. On the 14th Moscow used "Carrots", Rostov "Beans", and Krakow "Apple". Note: One such change occurred during the period of observation.

(2) MESSAGE SERIAL NO. Assigned by originating station. This number runs consecutively from day to day and does not revert to 1 at the beginning of each 24 hour period.

(3) DEPARTMENT (?). The exact significance of this portion of the preamble is not known. On some of the intercepted traffic it appeared as a letter and in several cases was totally absent. When used however, it seems to have some connection with the Message Serial No. (2).

(4) ? Name or purpose unknown but appears in every preamble preceding the group count (5 below).

(5) GROUP COUNT. Number of groups in text including indicator (9) and bloknot (10).

(6) DATE.

(7) TIME OF ORIGIN.

TOP SECRET "U"

Report on T/A of BAUDOT traffic (continued)

(8) ADDRESS, ROUTING INSTRUCTIONS AND PRIORITY. The length of this part of the preamble may consist of from 2 to 9 words. In the example given: 8a indicates "to cipher office" and is usually found in all messages preceding 8b, the cover name of the addressee; 8c is the priority. Note: Should this message have been relayed, the cover name of the relaying station would also appear here.

(9) INDICATOR. Normally found twice in each message, first group of the text if 5/L traffic, sixth group if 5/F. In both 5/F and 5/L traffic it appears as the last group of text before the Bloknot (10 below).

MESSAGE ENDING:

9	10	11	12	13
15019	58138	P.	DEMAMOVA	1323

(10) BLOKNOT. "One time pad" sheet (?) number. Because of its continuity from message to message and from day to day, this number along with the message serial is undoubtedly the most important and surest means of identifying a group.

(11) PEREDALA. (Russian for "sent by"). This word may appear in abbreviated form or in full.

(12) OPERATOR'S SIGNATURE. Always a proper name.

(13) TIME SENT. Note: One of the operators observed had a tendency to send this group preceding her signature. The standard practice however, is to transmit the time sent as the last group of the message.

4. GENERAL OBSERVATIONS

a. The bulk of the traffic intercepted on the 2-channel apparatus was 5/L and 5/F Military-- preambles and endings were substantially the same in both. The 6 and 9-channel apparatus passed commercial traffic in clear text and presented no T/A problem.

b. A few Police (SMERSH) messages were passed on the 2-channel apparatus.

c. No lateral working was noted.

d. No "Q" code or procedure signals were employed.

e. Frequencies used were all between 8000 and 11000 kcs. No pattern of frequency allocation could be discerned.

REPRODUCED AT THE NATIONAL ARCHIVES

TOP SECRET "U"

Report on T/A of BAUDOT traffic (continued)

f. Frequency changes occur at irregular intervals, the procedure for which seems amazingly simple. The operator requesting the shift transmits, "Will you change to ..... kcs, acknowledge by sending A-Z". Note: The number which precedes kcs. when divided by 25 gives the new frequency. The acknowledgment signal can be any word or letter which strikes the originating operator's fancy.

g. Operators' names provide an aid to the identification of subordinate subscribers. This is based on:

(1) Relayed messages are re-transmitted with the originating station's cover name in position 1 of the preamble.

(2) The relaying station's cover name appears in position 8.

(3) The operator at the relaying station signs the transmission.

5. CONCLUSIONS

a. A clear W/T picture can be obtained by a careful study and card indexing of even the smallest detail serving to characterize the traffic. Cover names, message serials, operators' names and bloknot numbers are of particular importance in this connection.

b. If an efficient standard of interception is to be maintained, the T/A processes required should be undertaken at the intercept station, in the closest possible collaboration with the set room.

c. Experienced Traffic Analysts could quickly adapt themselves to the Baudot problem with a minimum amount of training. Two of the essentials in such training would be a familiarization with the Russian Alphabet and some 50 odd phrases common to the traffic.

d. At least one fluent Russian speaker should be present at all times to deal with plain language chat.